ELSEVIER

Discrete Mathematics 208/209 (1999) 299–309

DISCRETE MATHEMATICS



# On the number of directions determined by a point set in AG(2, $p$)

András Gács

*Institute of Mathematics, Hungarian Academy of Sciences, H-1053, Budapest, Reáltanoda u. 13-15, Hungary*

Received 5 March 1997; revised 14 April 1998; accepted 11 May 1998

**Abstract**

It has been known for a long time that a $p$-element point set in AG(2, $p$), which is not a line, determines at least $(p+3)/2$ directions (Rédei, Lückenhafte Polynome über endlichen Körpern, Birkhauser Verlag, Basel, 1970 (English translation: Lacunary Polynomials over Finite Fields, North-Holland, Amsterdam, 1973)). In this paper we look for sets determining more than $(p+3)/2$ directions. We prove that besides two examples no set determines $(p+5)/2$ directions, give an infinite series of examples determining $7p/9$ directions approximately and prove results about the graph of monomials. These results suggest a conjecture, namely that no point set can determine $N$ directions with $(p+3)/2 < N < 2p/3$. 

## 1. Introduction

Throughout this paper $U = \{(a_i, b_i)\colon i = 1, \ldots, q\}$ will denote a $q$-element point set in AG$(2, q)$, the Desarguesian affine plane of order $q$.

**Definition 1.1.** We say that $U$ determines the direction $m \in \mathrm{GF}(q) \cup \{\infty\}$ if $m = (b_i - b_j)/(a_i - a_j)$ for suitable $i \neq j$, and denote by $D$ the set of determined directions. Finally let $N = |D|$, the number of determined directions.

The problem of determining the possible values of $N$ and characterizing the corresponding point sets is important for at least two reasons. The first is that it has applications to the theory of permutation polynomials, which we shall discuss in the next section. The second reason is its connection with blocking sets.

*E-mail address:* gacs@cs.elte.hu (A. Gács)

0012-365X/99/$ - see front matter 
PII: S0012-365X(99)00078-3

A *blocking set* in a projective plane is a point set meeting every line, but containing no line. A way to construct a blocking set in $\mathrm{PG}(2,q)$ is to take a $q$-element point set $U$ in $\mathrm{AG}(2,q)$ and add all infinite points corresponding to the directions it determines. In this way, we get a blocking set of size $q+N$ with the property that there is a line (namely the line at infinity) meeting the blocking set in all but $q$ points. Blocking sets arising this way are called of *Rédei-type*. For more information, we refer to [3].

After results of Rédei [9] and Lovász and Schrijver [7], recently the problem of determining the possible values of $N$ and characterizing the corresponding point sets has been almost completely solved by Blokhuis et al. [1] for the case when the number of determined directions is less than $(q+3)/2$, that is essentially all Rédei-type blocking sets of size less than $q+(q+3)/2$ have been classified.

For $q=p$ prime, there is no example in this case:

**Theorem 1.2** (Lovász–Schrijver [7]). *If a point set in* $\mathrm{AG}(2,p)$ *is not a line, then it determines at least* $(p+3)/2$ *directions with equality if and only if it is affinely equivalent to the graph of the polynomial* $f(x)=x^{(p+1)/2}$. □

With the blocking set terminology, this result says that Rédei-type blocking sets in $\mathrm{PG}(2,p)$ have size at least $p+(p+3)/2$, and there is an essentially unique example attaining equality in the bound. In the prime case the first part of this is true about all blocking sets:

**Theorem 1.3** (Blokhuis [2]). *In* $\mathrm{PG}(2,p)$ *a blocking set has size at least* $p+(p+3)/2$. □

Besides one example in the plane of order 7, the only known blocking set of minimum size in $\mathrm{PG}(2,p)$ is the one of Rédei type, there are results suggesting that no other example exists, see [4,6].

In this paper we deal with point sets in $\mathrm{AG}(2,p)$, $p$ prime. All results will be formulated in the affine terminology, that is with $p$-element sets and directions, but a corresponding result is always true for blocking sets (of Rédei-type).

We are going to prove that apart from two examples, no set determines $(p+5)/2$ directions (Theorem 5.1), give an infinite series of examples determining $7p/9$ directions approximately and prove results about the graph of monomials. These results suggest a conjecture, namely that no point set can determine $N$ directions with $(p+3)/2 < N < 2p/3$.

## 2. Permutation and complete mapping polynomials

A polynomial is called a *permutation polynomial* if it is bijective as a function over the field. The following propositions show the connection between our problem and permutation polynomials.

**Proposition 2.1.** *If a set does not determine all directions, then after a suitable affine transformation* (*which does not affect the number of directions*), *it can be taken as the graph of a polynomial.*

**Proof.** Since every function is a polynomial over a finite field, the only thing we need is that $\infty$ is not a determined direction, this can be achieved. □

We say that a polynomial determines a direction if its graph determines it.

The interesting case will always be when the number of determined directions is at most $p-2$. Thus we can suppose $p \geqslant 11$: otherwise $(p+3)/2 \geqslant p-2$, so according to Theorem 1.2, there are no more examples.

The use of considering polynomials can be seen through the following statement:

**Proposition 2.2.** *If the set in question is the graph of the polynomial $f(x)$, then the direction $c$ is determined if and only if $f(x)-cx$ is not a permutation polynomial.*

**Proof.** The direction $c$ is determined if and only if $c=[f(x_1)-f(x_2)]/[x_1-x_2]$ for suitable $x_1 \neq x_2$, which is equivalent to saying that $f(x_1)-cx_1 = f(x_2)-cx_2$, that is $f(x)-cx$ takes a value twice, so it cannot be a permutation. □

This proposition will be used in conjunction with the following statement:

**Proposition 2.3.** (i) *If $f(x)=c_{p-1}x^{p-1}+\cdots+c_0$, then $\sum_{x\in \mathrm{GF}(p)} f(x) = -c_{p-1}$.*

(ii) *If $f(x)$ is a permutation polynomial, then for all $1 \leqslant k \leqslant p-2$, $f(x)^k$ has degree at most $p-2$ when reduced modulo $(x^p-x)$.*

**Proof.** (i) $\sum_x f(x) = \sum_x \sum_{i=0}^{p-1} c_i x^i = \sum_{i=0}^{p-1} c_i \sum_x x^i = -c_{p-1}$.

(ii) If $f(x)$ is bijective, then $\sum_{x\in \mathrm{GF}(p)} f(x)^k = \sum_{x\in \mathrm{GF}(p)} x^k = 0$ for $1 \leqslant k \leqslant p-2$. This together with (i) completes the proof. □

There is another notion which connects directions and polynomials. The polynomial $f(x)$ is called a *complete mapping polynomial* if $f(x)$ and $f(x)+x$ are both permutations. Note that this is equivalent to a point set not determining the directions $\infty, 0$ and $-1$. For more about complete mapping polynomials, we refer to [8]. We only mention a result of Cohen [5], which is equivalent to stating that non-linear small degree polynomials determine all but maybe one direction.

**Theorem 2.4.** *Over a prime field there are no complete mapping polynomials of degree $n \geqslant 2$ for which $(n^2-3n+4)^2 < p$ holds.* □

## 3. Examples

In this section we give the known and some new examples for sets determining less than $p-1$ directions. The order of the field will be denoted by $p$, though all

constructions work over an arbitrary finite field. The first infinite series is due to Megyesi.

**Example 3.1.** Let $G$ be a multiplicative subgroup of the field GF($p$) with $|G| = d$ (so $d|p-1$ holds). Define the point set as

$$U = \{(0,0)\} \cup \{(x,0): x \in G\} \cup \{(0,x): x \notin G\},$$

that is we put $G$ on the horizontal axis and the complement of $G$ on the vertical axis together with the origin. It is easy to see that $D = \{\infty, 0\} \cup (\mathrm{GF}(p)^* \setminus G)$, that is $N = p + 1 - d$. □

This example has the property that it is contained in the union of two lines. The following result was conjectured by Cameron and finally proved by Szőnyi:

**Theorem 3.2.** *If $U$ is contained in the union of two lines and $N < p-1$, then after a suitable linear transformation*

$$U = \{(0,0)\} \cup \{(x,0): x \in K\} \cup \{(0,x): x \notin K\},$$

*where $K$ is the union of some cosets of a multiplicative subgroup of* GF($p$) *and $N = p + 1 - d$, where $d$ is the order of the subgroup in question.*

**Proof.** See [10]. □

The following examples are similar to the previous one: this time we put three cosets of a multiplicative subgroup on three lines.

**Example 3.3.** Suppose $3|p-1$ and let $G$ be the multiplicative subgroup of GF($p$) of order $(p-1)/3$. Let $G$, $\alpha G$ and $\alpha^2 G$ be the three cosets of $G$ in GF($p$)$^*$. We define three sets:

$$U_1 = \{(0,0)\} \cup \{(x,0): x \in G\} \cup \{(x,x): x \in G\} \cup \{(0,x): x \in G\},$$

$$U_2 = \{(0,0)\} \cup \{(x,0): x \in \alpha G\} \cup \{(x,x): x \in G\} \cup \{(0,x): x \in \alpha G\},$$

$$U_3 = \{(0,0)\} \cup \{(x,0): x \in \alpha^2 G\} \cup \{(x,x): x \in G\} \cup \{(0,x): x \in \alpha^2 G\},$$

Denote by $D_i$ and $N_i$ the set and the number of determined directions of $U_i$ ($i = 1,2,3$), respectively.

Before calculating $D_i$ and $N_i$, we introduce some notation and prove a lemma.

For any subset $K$ of GF($q$), let $-K = \{-x: x \in K\}$, $K + 1 = \{x + 1: x \in K\}$ and $1/K = \{1/x: x \in K\}$. In the third case the resulting set might contain $\infty$. Note that $G = -G$.

**Lemma 3.4.** *For any* $g \neq 0$, $G \cap (1-gG) = G \cap 1/(1-gG) = (1-gG) \cap 1/(1-gG)$.

**Proof.** We show $G \cap (1-gG) \subseteq G \cap 1/(1-gG) \subseteq (1-gG) \cap 1/(1-gG) \subseteq G \cap (1-gG)$.

Let $x \in G \cap (1-gG)$, that is $x = 1 - gy$ with $y \in G$. Dividing by $x$ one gets $1 = 1/x - gy/x$, implying $x = 1/[1 - g(-y/x)] \in 1/(1-gG)$.

Next let $x = 1/(1-gy) \in G \cap 1/(1-gG)$. This implies $1 - x = g(-yx) \in gG$, so $x = 1 - (1-x) \in 1 - gG$.

Finally, if $1 - gx = 1/(1-gy)$, then $(1-gx)(1-gy) = 1$, which implies $1/(1-gy) = -x/y \in G$. □

**Proposition 3.5.** (i) $D_1 = G \cup (1-G) \cup 1/(1-G)$, $N_1 = p - 1 - 2|G \cap (G+1)|$.

(ii) $D_2 = \{\infty, 0\} \cup G \cup (1-\alpha G) \cup 1/(1-\alpha G)$, $N_2 = p + 1 - 2|\alpha G \cap (G+1)|$.

(iii) $D_3 = \{\infty, 0\} \cup G \cup (1-\alpha^2 G) \cup 1/(1-\alpha^2 G)$, $N_3 = p + 1 - 2|\alpha^2 G \cap (G+1)|$.

**Proof.** The calculation of $D_i$ is easy for all the three cases.

To calculate $N_i$, one should use the previous lemma and inclusion–exclusion. Finally note that $|G \cap (1-G)| = |G \cap (G+1)|$, $|G \cap (1-\alpha G)| = |\alpha G \cap (1+G)|$, and $|G \cap (1-\alpha^2 G)| = |\alpha^2 G \cap (1+G)|$. □

The following two statements together show that in fact each set determines $7p/9$ directions, approximately.

**Proposition 3.6.** $N_1 + N_2 + N_3 = 3p + 1 - 2(p-1)/3$.

**Proof.** $(1+G) \setminus \{0\}$ is the disjoint union of $(1+G) \cap G$, $(1+G) \cap \alpha G$ and $(1+G) \cap \alpha^2 G$. □

**Proposition 3.7.** $N_i = 7p/9 + O(\sqrt{p})$.

**Proof.** We give the proof for $i = 1$, the other two cases are similar.

Note that $G = \{x^3 : x \in \mathrm{GF}(p)^*\}$, so $|G \cap (G+1)| = |\{(x^3, y^3) \in \mathrm{GF}(p)^* \times \mathrm{GF}(p)^* : x^3 - y^3 - 1 = 0\}| = 1/9|\{(x,y) \in \mathrm{GF}(p)^* \times \mathrm{GF}(p)^* : x^3 - y^3 - 1 = 0\}|$.

Now $x^3 - y^3 - 1 = 0$ is an absolutely irreducible plane curve of degree 3, so according to Weil's estimate, the number $S$ of its $\mathrm{GF}(p)$-rational points can be estimated as follows:

$$p - (3-1)(3-2)\sqrt{p} \leqslant S \leqslant p + (3-1)(3-2)\sqrt{p} + 1.$$

The difference between $S$ and $|\{(x,y) \in \mathrm{GF}(p)^* \times \mathrm{GF}(p)^* : x^3 - y^3 - 1 = 0\}|$ is at most 9 (the number of possible solutions with $x = 0$ or $y = 0$ plus the number of infinite points of the curve), so we get

$$|\tfrac{9}{2}(p - 1 - N_1) - p| \leqslant 2\sqrt{p} + 10,$$

which clearly yields

$$\left|\frac{7p}{9} - N_1\right| \leqslant \frac{4\sqrt{p}}{9} + 4. \qquad \square$$

**Remark 3.8.** The following example also gives around $7p/9$ directions, we omit the details:

$$U = \{(0,0)\} \cup \{(x,0): x \in \alpha G\} \cup \{(x,x): x \in G\} \cup \{(0,x): x \in \alpha^2 G\}.$$

## 4. The number of directions determined by a monomial

In this section we deal with the case when the point set in question is the graph of a monomial. Recall that the extremal case in Theorem 1.2 is achieved by a monomial. Also note that the graphs of the polynomials $x^{(p+2)/3}$ and $x^{(2p+1)/3}$ are always one of the examples described in the previous section.

**Proposition 4.1.** *Let* $2 \leqslant n \leqslant p-1$ *and suppose one of the following holds*:

(i) $(n-1, p-1) = 1$,
(ii) $n \leqslant \sqrt{p-1}$,
(iii) $n \geqslant p - \sqrt{p}$,
(iv) $(p-1)/2 - (\sqrt{p-1})/2 < n \leqslant (p-1)/2$,
(v) $(p+3)/2 \leqslant n \leqslant (p-1)/2 + \sqrt{(p-1)/2}$.

*Then the polynomial* $f(x) = x^n$ *determines* $p-1$ *or* $p$ *directions, according as* $(p-1, n) = 1$ *or* $(p-1, n) > 1$.

**Proof.** $f$ determines the direction 0 if and only if it is not a permutation, that is exactly when $(p-1, n) > 1$, so what we need is that $f(x) + mx$ cannot be a permutation for $m \neq 0$. We prove this using Proposition 2.3.

Write $p - 1 = an + b$ with $0 \leqslant b < n$ and consider $(f(x) + mx)^{a+b}$:

$$(x^n + mx)^{a+b} = \sum_{k=0}^{a+b} \binom{a+b}{k} x^{nk} x^{a+b-k} m^{a+b-k}$$

$$= \sum_{k=0}^{a+b} \binom{a+b}{k} m^{a+b-k} x^{kn+a+b-k},$$

so the degree of a typical term is $a'n + b'$, with $a' + b' = a + b$. For $a' = a$, we get $an + b = p - 1$. (Note that since $p$ is a prime, the binomial coefficients are not zero.) Suppose there is another term, $x^{a'n+b'}$ say, giving $x^{p-1}$ modulo $(x^p - x)$. This gives $p - 1 | (a - a')(n - 1)$. We show case by case, that this can only hold for $a = a'$, so the degree of $(f(x) + mx)^{a+b}$ is $p - 1$. Note that $|a - a'| \leqslant \max(a, b)$.

Table 1
List of values of $p, n$ and $N$, s.t. $11 \leqslant p \leqslant 100$ and $x^n$ determines $N$ directions with $(p+5)/2 \leqslant N \leqslant p-2$

| $p$ | $n$ | $N$ | $p$ | $n$ | $N$ |
|---|---|---|---|---|---|
| 19 | 7 | 15 | 61 | 41 | 48 |
| 19 | 13 | 15 | 61 | 46 | 57 |
| 29 | 8 | 25 | 67 | 23 | 54 |
| 31 | 11 | 24 | 67 | 45 | 55 |
| 31 | 21 | 25 | 73 | 19 | 68 |
| 31 | 25 | 26 | 73 | 25 | 57 |
| 37 | 13 | 33 | 73 | 49 | 57 |
| 37 | 25 | 33 | 73 | 55 | 64 |
| 37 | 28 | 33 | 79 | 27 | 67 |
| 43 | 15 | 37 | 79 | 53 | 66 |
| 43 | 29 | 36 | 89 | 67 | 76 |
| 53 | 40 | 49 | 97 | 25 | 92 |
| 61 | 13 | 55 | 97 | 33 | 73 |
| 61 | 16 | 57 | 97 | 65 | 72 |
| 61 | 21 | 49 | 97 | 73 | 92 |
| 61 | 37 | 55 | | | |

Suppose (i) holds. Then $p-1|(a-a')$, which implies $a=a'$, since otherwise $p-1 \leqslant |a-a'| \leqslant \max(a,b)$ would hold.

If (ii) is true, then $a \geqslant b$, so for $a-a' \neq 0$, we get $p-1 \leqslant |a-a'|(n-1) \leqslant a(n-1) < an+b = p-1$, a contradiction.

If (iii) holds, then $a=1$, $\max(a,b) \leqslant \sqrt{p}-1$ and $(n-1, p-1) \leqslant p-n \leqslant \sqrt{p}$, so again $a \neq a'$ would imply $p-1 \leqslant |a-a'|(p-1, n-1) \leqslant p-\sqrt{p}$.

Next suppose (iv) and write $n=(p-1)/2-s$. For $s=0$, the claim is obvious so let us assume $s>0$. It is easy to see that $a=2$, $b=2s$ and $\max(a,b)=2s$. $(p-1,n) \leqslant (p-1,2n) \leqslant p-1-2n=2s$, so $a \neq a'$ would imply $b*2s=(2s)^2 \geqslant p-1$.

The only remaining case is (v). Write $n=(p-1)/2+s$. We redefine $a$ and $b$ as follows: let $a$ be odd and $b \leqslant 2s-1$, s.t. $as+b=(p-1)/2$. It is easy to see that $(f(x)+mx)^{a+b}$ still has a term, namely $f(x)^a x^b$, which reduces to $x^{p-1}$. If another term, $f(x)^{a'}x^{b'}$ say, had the same property, then we would have $p-1|(a-a')(n-1)$ just like in the previous cases, which now implies $(p-1)/2|(a-a')(s-1)$. This is impossible for $a \neq a'$. □

**Remark 4.2.** It would be easy to generalize Proposition 4(iv) and (v) to a statement for $n$ near to $(p-1)/d$, but not equal $(p-1)/d+1$.

**Remark 4.3.** Note that with the terminology of the second section, Proposition 4.1 means that there are no monomial complete mapping polynomials of the form $ax^n+b$ with $ab \neq 0$ and $n$ satisfying any of (i)–(v). This generalizes (for prime fields) a result in [8] stating that there are no monomial complete mapping polynomials of degree $n \geqslant 2$, with $(n^2-4n+6)^2 < p$.

We are going to prove the following theorem in the next section:

**Theorem 4.4.** *Let $f(x)=x^n$ be a monomial. If $f$ is not linear and $n \neq (p+1)/2$, then $f$ determines at least $(2p+2)/3$ directions.* □

The previous two results suggest that monomials do not give too many examples. However, as it can be seen in Table 1, this is not so.

Note that for all but one example ($p=61, n=37, N=55$), $n-1 \mid p-1$ or $p-n \mid p-1$ holds.

## 5. The general case

Throughout this section $f(x)=c_{p-1}x^{p-1}+\cdots+c_0$ will be a reduced polynomial over GF($p$) of degree $n$. We are going to prove bounds on $N$ (the number of directions $f$ determines), depending on $n$. Besides Theorem 4.4 our main result will be the following:

**Theorem 5.1.** *Suppose $f$ determines $(p+5)/2 < p-1$ directions. Then $p=11$ and $f(x)$ is affinely equivalent to one of the following polynomials: $x^7+x^5+5x^3$ or $x^7-x^5+5x^3$.*

The following result can be found in [7].

**Proposition 5.2.** *If $f$ determines $N$ directions, then $\Sigma_{k,l} := \Sigma_{x\in \mathrm{GF}(p)} x^k f(x)^l = 0$ for all $1 \leqslant k+l \leqslant p-N$.* □

This statement needs some explanation. First of all, if $k=0$ or $l=0$, then calculating the double power sum, $0^0$ may occur, which is defined to be 1. Note that according to Proposition 2.3, $-\Sigma x^k f(x)^l$ is the coefficient of $x^{p-1}$ in $x^k f(x)^l$ after reduction modulo $(x^p-x)$.

The following was probably first noticed by W.S. Chou:

**Proposition 5.3.** *If $f$ determines $N$ directions, then $n \leqslant N-1$.*

**Proof.** From Proposition 5.2 we have $\Sigma f(x)x^k = 0$ for $k=0,\ldots,p-N-1$, giving $c_{p-1}=\cdots=c_N=0$. □

**Proposition 5.4.** *If $2 \leqslant n \leqslant (p-1)/2$, then $f$ determines at least $p+1-(p-1)/3$ directions for $n \neq (p+1)/3$ and at least $p+1-(p+1)/3$ directions for $n=(p+1)/3$.*

**Proof.** Note that for $n=2$ or 3, $f$ is affinely equivalent to a monomial, so we can use Proposition 4.1.

Suppose $n \geqslant 4$ and write $p-1=an+b$ with $b \leqslant n-1$. Since $f(x)^a x^b$ has degree $p-1$, using Proposition 5.2 it is enough to prove that $a+b \leqslant (p+1)/3$ or $a+b \leqslant (p-1)/3$ according as $n=(p+1)/3$ or not. For $p \leqslant 23$, a case by case analysis shows that the claim is true, so we can suppose $p \geqslant 29$.

$a+b \leqslant (p-n)/n+n-1$, so we need $p/n+n \leqslant (p+5)/3$. Multiplying with $n$, we see that the following quadratic inequality has to be satisfied: $n^2 - [(p+5)/3]n + p \leqslant 0$. With an easy calculation one sees that this is true for $p \geqslant 28$ and $4 \leqslant n \leqslant (p-7)/3$.

For $(p-6)/3 \leqslant n \leqslant (p-1)/3$ and $p \geqslant 28$, we have $a=3$, $b \leqslant 5$, so $a+b \leqslant 8 \leqslant (p-1)/3$.

For $n \geqslant (p+1)/3$, we have $a=2$, $b \leqslant (p-5)/3$ with equality if and only if $n=(p+1)/3$. □

**Proposition 5.5.** *Suppose $n=(p+1)/2$. Then $f$ is affinely equivalent to $x^{(p+1)/2}$ determining $(p+3)/2$ directions, or $f$ determines at least $3p/4$ directions.*

**Proof.** After affine transformation suppose $f(x) = x^{(p+1)/2} + g(x)$ with $s = \deg g \leqslant (p-3)/2$, $x^2 | g(x)$. For $s=0$, we have $f(x)=x^{(p+1)/2}$, so we are done by Theorem 1.2.

Suppose $s \geqslant 2$, write $(p-3)/2 = as+b$ and consider $f(x)^{a+1}x^b = g(x)^{a+1}x^b + (a+1)g(x)^a x^{(p+1)/2+b} + \cdots$. We claim that the only term giving $x^{p-1}$ after reduction is $g(x)^a x^{(p+1)/2+b}$. Take a typical term, $r(x) = g(x)^{a+1-k}x^{k(p+1)/2+b}$. For $k$ even, $r(x) = g(x)^{a+1-k}x^{b+k}$ modulo $(x^p - x)$, which has degree $(a+1-k)s+b+k = (p-3)/2 + s - (s-1)k < p-1$. For $k$ odd, we have $r(x) = g(x)^{a+1-k}x^{(p-1)/2+k+b}$ modulo $(x^p - x)$, which has degree $(p-3)/2 + s - (s-1)k < p-1$.

Now $a+b \leqslant 1/s(p-3/2-(s-1)) + s - 1 = (p-1)/2s + s - 2$. This is at most $(p+1)/4$ for $2 \leqslant s \leqslant (p+1)/4$. For $s \geqslant (p+2)/4$, $a+b \leqslant (p+1)/4$ obviously. □

**Proof of Theorem 4.4.** Due to the previous propositions, the only case we have to consider is $(p+3)/2 \leqslant n \leqslant p-1-(p+1)/3$. Let $n=(p-1)/2+s$ and write $(p-1)/2 = as+b$ with $a$ odd and $b \leqslant 2s-1$. Then $f(x)^a x^b = x^{a(p-1)/2+(p-1)/2} = x^{p-1}$ modulo $(x^p - x)$, so according to Proposition 5.2, we only need $a+b \leqslant (p+1)/3$ (if $3 | p-1$, then this automatically implies $a+b \leqslant (p-1)/3$). $a+b \leqslant 1/s((p-1)/2 - (2s-1)) + 2s - 1 = (p+1)/2s + 2s - 3$. It is easy to verify that this is at most $(p+1)/3$ for $2 \leqslant s \leqslant (p-1)/6$ (and $p \geqslant 11$). □

We believe that this result could be extended to the general case:

**Conjecture.** Let $U$ be a set of $p$ points in AG$(2, p)$. One of the following holds.

(i) $U$ is a line determining one direction.

(ii) $U$ is affinely equivalent to the graph of $x^{(p+1)/2}$ determining $(p+3)/2$ directions

(iii) $U$ determines at least $(2p+2)/3$ directions ($(2p+4)/3$ for $3 | p-1$). □

Note that Propositions 5.3–5.5 together yield that a possible counterexample is the graph of a polynomial of degree between $(p+3)/2$ and $(2p-1)/3$. Also note that

this would be sharp: the example in Proposition 2.1 with $d=(p-1)/3$ determines $(2p+4)/3$ directions.

Finally we prove Theorem 5.1.

**Proof of Theorem 5.1.** The proof will work only for $p\geqslant 19$, since we use the double power sums from Proposition 5.2 with $k+l\leqslant 7$, which means that we need $(p-5)/2\geqslant 7$. For the case $11\leqslant p\leqslant 17$, see the remark after the proof. Throughout the proof the degree of a polynomial will mean its reduced degree, that is its degree after reduction modulo $(x^p-x)$.

Using Propositions 5.3–5.5, we see that $n=(p+3)/2$. Using Proposition 5.2 with $l=2$, $k=0,1,\ldots$, and with $l=3$, $k=0,1,\ldots$, we get $\deg(f^2)\leqslant(p+5)/2$, $\deg(f^3)\leqslant(p+7)/2$. Let $f^2(x)=Ax^{(p+5)/2}+Bx^{(p+3)/2}+\cdots \pmod{(x^p-x)}$. Note that $A=-\Sigma_x x^{(p-7)/2}f(x)^2$ and $B=-\Sigma_x x^{(p-5)/2}f(x)^2$. Let $g_1(x)=f(x)-(A/2)x-(B/2)$. It is easy to see that $\deg(g_1^2)\leqslant(p+1)/2$. We distinguish three cases depending on the degree of $g_1^2$.

*Case* 1. $\deg(g_1^2)=(p+1)/2$. Choosing an appropriate $c$, one can achieve that for $g(x):=g_1(x+c)$, $g^2(x)=Cx^{(p+1)/2}+Dx^{(p-3)/2}+Ex^{(p-5)/2}+\cdots \pmod{(x^p-x)}$ holds. Redefine $\Sigma_{k,l}$ as the related double power sums of $g(x)$.

Now $\Sigma_{0,4}=\Sigma_{1,4}=0$ gives $D=E=0$. Let $g(x)=x^{(p+3)/2}+c_{(p+1)/2}x^{(p+1)/2}+\cdots+c_0$. Then $G(x):=g(x)-1/C(xg^2(x)+c_{(p+1)/2}g^2(x))=c_{(p-1)/2}x^{(p-1)/2}+c_{(p-3)/2}x^{(p-3)/2}+\cdots$. Now, the double power sums of $G$ are the linear combinations of the $\Sigma_{k,l}s$, so $\Sigma_x G^2(x)=\Sigma_x xG^2(x)=0$, giving $c_{(p-1)/2}=c_{(p-3)/2}=0$. But this means that using $\Sigma_{0,2}=\Sigma_{1,2}=\cdots=0$, we get $g(x)-c_1x-c_0=x^{(p+3)/2}+c_{(p+1)/2}x^{(p+1)/2}=x^{(p-1)/2}(x^2+c_{(p+1)/2}x)$. Write $(p-1)/2=2a+b$ with $a$ even, $b\leqslant 3$. Then $\Sigma_{b,a}\neq 0$, a contradiction.

*Case* 2. $(p-3)/2\leqslant\deg(g_1^2)\leqslant(p-1)/2$. This contradicts $\Sigma_{0,4}=\Sigma_{2,4}=0$.

*Case* 3. $\deg(g_1^2)\leqslant(p-5)/2$. Note that this means that $\deg(g_1^3)=(p+3)/2+\deg(g_1^2)$, so because of $\deg(g_1^3)\leqslant(p+7)/2$, we have $\deg(g_1^2)\leqslant 2$. But since $g_1^2(x)$ is a square for every $x$, this can only hold if $g_1^2(x)=cx^2 \pmod{(x^p-x)}$ with $0\neq c\in \mathrm{GF}(p)^2$. This means that the graph of $g_1$ is contained in the union of two lines, so $g_1$ has to determine $p+1-(p-1)/d$ directions with a suitable $d\,|\,p-1$ by Theorem 3.2, a contradiction. □

**Remark.** The previous proof is valid only for $p\geqslant 19$. For $p=11$, 13 or 17, one can use a computer to check every polynomial. Note that the polynomial in question can be chosen as follows: $f(x)=x^{(p+3)/2}+ax^{(p-1)/2}+bx^{(p-3)/2}+c_{(p-5)/2}x^{(p-5)/2}+\cdots+c_2x^2$, where the $c_i$'s are determined by $a$ and $b$ through the equations $\Sigma_{k,2}=0$, $k=0,1,\ldots$. Also one can suppose $a=0$, $a=1$ or $a$ is an arbitrary non-square in $\mathrm{GF}(p)$. For $p=11$ there are polynomials for wich all the corresponding double power sums are zero, but determining more that 8 directions.

**Acknowledgements**

The author acknowledges the financial support of COST Grant 3314/95 and OTKA Grants F-016302 and T-019367.

## References

[1] A. Blokhuis, S. Ball, A. Brouwer, L. Storme, T. Szönyi, On the number of directions determined by a polynomial, J. Combin. Theory Ser. A 86 (1999).
[2] A. Blokhuis, On the size of a blocking set in $PG(2, p)$, Combinatorica 14 (1994) 111–114.
[3] A. Blokhuis, A.E. Brouwer, T. Szönyi, The number of directions determined by a function $f$ on a finite field, J. Combin. Theory Ser. A 70 (1995) 349–353.
[4] A. Blokhuis, R. Pellikaan, T. Szönyi, Blocking sets of almost Rédei-type, J. Combin. Theory Ser. A 78 (1997) 141–150.
[5] S.D. Cohen, Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials, Can. Math. Bull. 33 (1990) 230–234.
[6] A. Gács, A remark on blocking sets of almost Rédei-type, J. Geom. 60 (1997) 65–73.
[7] L. Lovász, A. Schrijver, Remarks on a theorem of Rédei, Studia Sci. Math. Hungar. 16 (1981) 449–454.
[8] P. Niederreiter, K.H. Robinson, Complete mappings over finite fields, J. Austral. Math. Soc. Ser. A. 33 (1982) 197–212.
[9] L. Rédei, Lückenhafte Polynome über endlichen Körpern, Birkhäuser Verlag, Basel, 1970 (English translation: Lacunary Polynomials over Finite Fields, North-Holland, Amsterdam, 1973).
[10] T. Szönyi, Combinatorial problems for Abelian groups arising from geometry, Period. Polytech. 19 (1991) 91–100.